Sähköpostin suodatus

Sähköpostin käsittelysäännöissä määritellään periaatteet, joilla sähköpostia välitetään. Tässä ohjeessa täsmennetään, miten sähköpostiviestejä yliopistossa suodatetaan. Suodatuksen tulee aina tapahtua ohjelmallisesti ja viestintäsalaisuuden säilyttäen.

Tämä ohje on julkinen ja sen tulee olla julkisesti saatavilla.

Koska haittaohjelmat ja roskapostit vaarantavat tietoturvallisuutta ja voivat jopa estää viestinnän, suodatetut viestit voidaan tapauskohtaisesti jättää välittämättä, tuhota tai poistaa liite, eristää erilliselle karanteenialueelle määräajaksi, jonka jälkeen ne tuhotaan, tai välittää vastaanottajalle roskapostiksi merkittynä. Haittaohjelmat tulee aina pyrkiä poistamaan välitettävistä viesteistä. Suodatetuista viesteistä lähettäjälle tai lähettävälle postipalvelimelle ja/tai vastaanottajalle lähetettävien virheilmoitusten tulee olla RFC 2821 -standardin mukaisia. Virheilmoitukseen voidaan myös liittää käyttäjäystävällinen kuvaus virheestä silloin, kun se on mahdollista.

Suodatusmenetelmät

Third party open relay -esto, eli releointihyökkäysten esto yliopiston koneiden kautta
Yliopisto ei välitä ulospäin sellaisia viestejä, jotka eivät ole lähtöisin yliopiston osoiteavaruudesta ja joiden vastaanottajan osoite ei ole yliopiston sähköpostiosoite. Lisäksi yliopisto estää palomuurikonfiguraatiossaan SMTP-yhteydet muihin kuin pääasiallisiin postipalvelimiinsa internetistä käsin. Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: -550 Relaying denied-

Postin välitys tuntemattomista toimialueista tai koneista
Yliopiston postipalvelin tekee nimipalvelutarkastuksen lähettäjätoimialueen tai -koneen olemassaolon varmistamiseksi. Mikäli lähettävä toimialue tai kone ei selviä nimipalvelukyselystä, voidaan postitus estää tilapäisesti kunnes lähettävän koneen tai toimialueen nimipalvelutietueet ovat kunnossa. Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: -451 Sender domain must resolve-

Mustat listat (Black Lists)
Yliopisto ei välitä postia sellaisista postikoneista, joita voidaan käyttää releointihyökkäyksiin (ks. kohta 1). Yliopisto saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja. Esimerkkejä alla:

- MAPS (Mail Abuse Prevention System)
- ORDB (Open Relay DataBase)
- DSBL (Distributed Server Boycott List)
- SPAMHAUS (The Spamhaus Project)

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: -550 Mail from rejected as spam; see http://www.käytettävä_musta_lista.domain-

Postin välitys sellaisista postikoneista, joiden kautta tunnetusti lähetetään roskapostia

Yliopisto ei välitä postia sellaisista koneista, joiden kautta tunnetusti lähetetään roskapostia tai joita ylläpitävä organisaatio tunnetusti tukee roskapostittajia. Tähän organisaatio saa käyttää apunaan kansainvälisten, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja. Esimerkiksi NJABL-tietokantaa (Not Just Another Bogus List).

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: -550 Mail from rejected as spam; see http://www.njabl.org-

Postin välitys sellaisista koneista, joilla on dynaamisesti varattu verkko-osoite
Yliopistolla on oikeus olla välittämättä postia sellaisista koneista, joiden verkko-osoite kuuluu dynaamisesti varattaviin osoiteavaruuksiin. Yliopisto saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja, esimerkiksi NJABL Dynablock.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: -550 Mail from rejected as spam; see http://www.njabl.org/dynablock.html".

Yliopisto saa käyttää tarkastuksessa apunaan kansainvälisiä, tunnettujen palveluntarjoajien ylläpitämiä tietokantoja. Tietokantoja käytettäessä tulee varmistua niiden asianmukaisuudesta mm. tarkastamalla periaatteet, joilla osoitteita kantaan lisätään. Tietokantoja ylläpitävän palveluntarjoajan on tarjottava helppokäyttöinen mekanismi, jolla osoitteita voi pyytää poistettavaksi kannasta. Poistopyynnöt on käsiteltävä kohtuullisen ajan kuluessa niiden tekemisestä. Tietokantoja käytettäessä tarkastus voi olla reaaliaikainen tai yliopisto voi ylläpitää omaa kopiotaan tietokannoista, jota kuitenkin tulee päivittää kohtuullisin väliajoin.

Palvelinkohtainen pääsylista
Yliopisto käyttää tarvittaessa haittapostin torjumiseen itse ylläpitämiään palvelinkohtaisia pääsylistoja (access list). Listan avulla voidaan sulkea tilapäisesti tai pysyvästi erillisiä toimialueita, lähettäjiä, vastaanottajia, yksittäisiä verkko-osoitteita tai kokonaisia aliverkkoja, mikäli se on välttämätöntä muun liikenteen turvaamiseksi tai yksittäisen henkilön häirinnältä suojaamiseksi.

Esimerkki lähettävälle postipalvelimelle toimitettavasta virheilmoituksesta: -550 Mail from rejected as spam- tai -550 Access Denied-

Liikennemääriin perustuva suodatus
Liikenneanalyysisuodatuksessa voidaan esimerkiksi sähköpostipalvelimen lokeja reaaliaikaisesti tarkkailemalla huomata poikkeamat normaalissa postinkulussa. Tällaisia roskapostitukseen viittaavia poikkeamia voivat olla epätavallisen pitkät yhteysajat postipalvelimeen, poikkeuksellinen määrä viestejä samasta isännästä tai suuri määrä vastaanottajia samassa viestissä. Liikennemääriä voi kontrolloida myös proaktiivisesti esimerkiksi hidastamalla yhteysnopeuksia tai rajoittamalla yhteysaikaa. Rajoituksia tulee kuitenkin aina käyttää harkiten, jotta esimerkiksi sähköpostilistojen toiminta ei häiriytyisi.

Viestien koko ja liitetiedostojen määrä
Yliopistolla on oikeus rajoittaa välittämiensä viestien kokoa ja niiden mahdollisesti sisältämien liitetiedostojen määrää. Tiedon viestin kokoon ja liitetiedostojen määrään liittyvistä rajoituksista tulee olla julkisesti saatavilla.

Haittaohjelmien poistaminen
Yliopisto poistaa välittämistään viesteistä haittaohjelmat mahdollisuuksiensa mukaan tai tarpeen vaatiessa tuhoaa koko haittaohjelman sisältävän viestin.

Liitetiedostojen tiedostotyypit
Yliopistolla on oikeus olla vastaanottamatta / välittämättä riskialttiita, haittaohjelmien kuljetukseen tyypillisesti käytettäviä tiedostotyyppejä sisältäviä viestejä.

Esimerkkejä tiedostotyypeistä.
*.ade, *.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.dll, *.exe, *.hlp, *.hta, *.inf, *.ins, *.isp, *.js, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.ocx, *.pcd, *.pif, *.reg, *.scr, *.sct, *.shs, *.url, *.vb, *.vbe, *.vbs, *.wsc, *.wsf, *.wsh

Ajantasainen lista tiedostotyypeistä, joita yliopiston postipalvelin ei vastaanota/välitä, tulee aina olla julkisesti saatavilla. Välittämättä jätettävät tiedostot voidaan eristää määräajaksi karanteenialueelle, jolloin ne saatetaan vastaanottajan tai lähettäjän tietoon ennen niiden tuhoamista. Tällöin tiedosto voidaan toimittaa vastaanottajalle tämän sitä pyytäessä, edellyttäen että tiedosto ei sisällä esim. haitalliseksi katsottua koodia.

Sähköpostin sisältöön perustuva suodatus
Yliopisto voi suodattaa roskapostia ohjelmallisesti sisällölliseen automaattiseen analyysiin perustuen, esimerkiksi pisteytykseen perustuvilla suodatusohjelmilla (esim. Spam Assassin, IMF).

Sisällöllisessä analyysissa roskapostiksi luokiteltu viesti tulee aina merkitä roskapostiksi ja toimittaa vastaanottajan sähköpostilaatikkoon, suodattaa erilliselle karanteenialueelle, josta se on vastaanottajan luettavissa, tai muutoin saattaa vastaanottajan tietoon kohtuullisen ajan kuluessa viestin vastaanottamisesta.

Viivästäminen
Yliopistolla on oikeus tarvittaessa viivästää viestien toimittamista kohtuullisen ajan tunnistaakseen mahdolliset liikenteen mukana tulevat haittaohjelmat.

Muuta
Yliopiston tulee palomuurikonfiguraatiossaan tai muutoin, mahdollisuuksiensa mukaan, estää sähköpostin lähettäminen muihin toimialueisiin muiden kuin virallisten postipalvelimiensa kautta.

Postin suodatusta on mahdollista tehdä sähköpostiohjelmaan asennettavassa lisäohjelmassa, keskitetyssä suodatuspalvelimessa tai yhdyskäytävässä. Suodatusohjeen kohdat 1-8 suositellaan tehtäväksi jo sähköpostiyhdyskäytävässä, kohta 9 keskitetyssä suodatuspalvelimessa ja käyttäjän työasemalla, kohta 10 keskitetyssä suodatuspalvelimessa sekä kohta 11 keskitetyssä suodatuspalvelimessa ja / tai käyttäjän työasemalla.

Suodatussuosituksen tekohetkellä ei-suositeltaviksi suodatusmenetelmiksi katsottiin sellaiset menetelmät, jotka olennaisesti rajoittavat sähköposti-arkkitehtuurin luontaista avoimuutta, esim. challenge/response, graylisting tai jotka ovat vielä toistaiseksi kokeellisessa käytössä, esim. RMX, SPF, DMP. Edellisten käyttö on hyväksyttävää arviointimielessä, mutta niitä ei tulisi

käyttää pääasiallisina suodatusmenetelminä.

Yliopiston tulee huolehtia siitä, että sähköpostitoimialueen ylläpitoon liittyvät sähköpostiosoitteet ovat olemassa ja että ne ohjautuvat oikealle taholle. Tällaisia osoitteita ovat mm. postmaster@tut.fi ja abuse@tut.fi.

Tiedon yliopiston käyttämistä suodatusmenetelmistä tulee aina olla julkisesti saatavilla.

Lisätietoa saa osoitteesta postmaster@tut.fi.